09-51

pennsylvania
OFFICE OF ADMINISTRATION

PUBLIC SAFETY RADIO SERVICES

September 23, 2009

Ms. Jennifer A. Manner
Deputy Chief
Public Safety and Homeland Security Bureau
Federal Communications Commission
Washington, DC 20554

Dear Ms. Manner:

Prior to my present job as head of the Commonwealth of Pennsylvania's digital radio network, I spent 33 years in the Philadelphia Police Department where I retired as a Deputy Police Commissioner. Many of the answers below come from a combination of the roles I played in both agencies.

<u>Questions</u>

What public safety applications must be offered as mission critical standards of quality and does that include broadband communications?

From the law enforcement side, the access to state, local and federal databases (those maintained by the FBI) are critical. Most of these applications don't really require a broadband connection. There is a need for broadband communications for some public safety applications and these are addressed in the questions below.

In an emergency what can be considered lower priority, voice or data?

There is no doubt that data will be of lower priority in an emergency and most LMR systems which combine voice and data will always give priority to voice over data if there is contention. Not every public safety agency has the ability to send and receive data transmissions but virtually all have the ability to listen to and respond to a radio call.

Besides video, which public safety application has the highest required data rate, and what is it? Which has the highest sustained bandwidth requirement?

I would like to preface this with some additional background. When public safety entities started to use wireless applications, the applications were largely queries of databases with text returned to the screen. These same applications today are still largely the 'bread and butter' of law enforcement wireless data. In recent years, there has been more text returned (not a problem even for low speed data bandwidth) but now more and more applications are accompanied by photos. Again, staying on the law enforcement side, these photos might be of a wanted suspect, missing child, license photo or a piece of stolen merchandise. Photos in and of themselves do not necessarily require a broadband connection. For example, we do well in PA with a 19.2 connection for delivering photos from driver's licenses to state police cars. The photos aren't large but they are adequate.

The other development in recent years which could substantially mitigate the need for high bandwidth is the increasing size of disk space accompanied with the steep price drop of storage. A terabyte of space can now be purchased for about $100. The first PC hard disks had a capacity of 10 megabytes and a cost of over $100 per MB. Modern hard disks with capacities of 100 gigabytes are common with a cost of less than 1 cent per MB. This represents an improvement of 1,000,000% in just under 20 years, or around 67% *cumulative* improvement per year. At the same time, the speed of the hard disk and its interfaces has increased dramatically as well.

What this means for public safety today is that an officer can carry information resident on a wirelessly enabled PC which only a few years had to be pushed to the same PC because there was no room to store it. If public safety applications are written which take advantage of the huge amounts of space on present day hard drives, information can be resident with the application only adding or subtracting information. Using this idea, a one terabyte drive can hold over 200,000 high quality photos of suspects (over a million lower quality photos). As suspects are captured, their photos would be removed by the application and only new suspects need be added. The bandwidth requirement for such an application would be relatively small. From an officer's perspective, the response for a suspect photo would be instantaneous since it would be resident on the hard drive. The same concept can be used for mapping applications which are now coming into vogue. CAD data for buildings or structures (drawings or photos) can be resident on the PC and updates sent and received in much the same way as with wanted photos.

The real drive for broadband for the police will come from 4 applications. The first is at the scene of either an emergency or pre-planned large event. There will be a need to move data around to the various participants at these types of events. Data may be in the form of video, pictures, large files or email (with or without large files attached). The second source will be in the area of identification. Law Enforcement will move toward applications where fingerprints will need to be sent wirelessly from a patrol car (or the scene of a mass arrest in the field) to an AFIS (Automated Fingerprint Identification System) to either identify an individual an officer has stopped or to be able to process prisoners from the field before they are transported to holding facilities.

The third application some departments will want to implement is to be able to monitor an officer in the vehicle remotely. Many police departments already have cameras installed in their cars. The next logical step would be to have the video from those cameras monitored from a dispatch center when the officer announces he/she is stopping a vehicle. The final application will be the creation of broadband 'hot spots'. For example, if the local police station were a 'hot spot', when officers were reporting on duty, an application can be updating the databases on their hard drives with virus definitions, updating maps and photos, downloading changes in police and procedure, performing operating system updates, etc.

The first two ideas above will need broadband speeds and the third one will need high sustained broadband speeds for those departments that adopt it.

One other area which drives law enforcement is the data offered through the FBI databases, notably the National Crime Information Center (NCIC). A look at where they are moving is a good indicator as to what requirements law enforcement will need in the future. Largely, local and state law enforcement networks tend to mirror in their own systems what NCIC proposes on a national basis.

During an emergency involving multiple public safety agencies operating over the same shared network, who should be in charge of determining which users or which traffic are allowed on the system and which have priority access?

The public safety agency with primary jurisdiction in the area of the emergency would be in charge. Most agencies would readily accept this. But the best policy is to have a joint command. The NIMS system recognizes this. Joint commands are almost always necessary because public safety agencies are extremely reluctant to take orders from an entity out of their normal chain of command.

How can Federal grant programs encourage equitable distribution of funding to create a more reliable national network for public safety, while making broadband deployment less complicated at the local level? Are there near and long term priorities that grants should target?

Federal grants in this arena should be formula grants and not competitive ones. Most entities won't argue about the size of the grant if the formula is fair. The money spent on the competitive process would be better spent on ensuring compliance by the grantees on the grant goals. Grants should be given to the states to be distributed by the Governor of the state to the areas which target the goals of the grant.

I am not in favor of building yet another network for public safety – a nationwide one no less. Why not meld existing state networks (and future ones being built) to do double duty in a sense? That duty would be to support the needs of the state and grants would be given to expand a state's existing network capabilities to provide access for other public safety responders (federal, state or local) who may come into or already operate within the state. For example, Pennsylvania has built one 800 MHz LMR network. Yet, we can use the same infrastructure to support VHF, UHF, 700 and broadband. We can also tie these disparate frequencies together so that anyone coming into the state can use them also. This idea accomplishes two goals. First it supports and builds comprehensive state networks furthering interoperability initiatives. Secondly it leverages those same networks which can be tied together to form one nationwide network. The costs are shared by both state and federal government to the benefit of both.

Sending broadband grants to the local level will inevitably result in a patchwork quilt of disparate networks which may or may not be able to work together. On the broadband issue, would you prefer to deal with 50 entities – one each at the state level, or thousands of entities if you include all the locals?

The most obvious near term task for public safety broadband is to identify the requirements. You are trying with these questions but I think we need a more structured approach. The vast majority of the public safety user community in the United States would say they needed broadband but not be able to identify one application outside of video in which broadband would be needed. As I mentioned at the panel discussion, I am not a fan of widespread video use but I do believe it has some limited use for public safety – not the ubiquitous use many would have you believe. Let's identify the requirements first, then the applications to fulfill those requirements. Only then will we really know the extent to which we will need broadband in the near future in public safety. It makes no sense to 'target' areas for broadband grants when the vast majority of users won't understand what they really need broadband for. Involving the vendor community in this effort is also necessary as they have done a poor job in educating public safety in the products and services they can offer in the broadband arena.

Do you envision a time when broadband communications will supplant legacy LMR emergency communications systems? What would need to happen in order for such an outcome to be achieved?

Others have brought this up and the question misses the point about what public safety LMR systems actually do. Broadband is the pipe – a large pipe. Public Safety LMR is an application which runs in the pipe. We will have bigger pipes in the future but there will always be the software running though them. Whether you call that software LMR or something else, it will be there nonetheless. The public safety LMR systems of today are all software driven and designed to public safety specifications. Radios are just mini computers. We are not going to move from these systems in the foreseeable future. The state of New York tried to sell the broadband idea to replace LMR and the concept died a very quick death.

LMR must be viewed as simply one application which can run on a broadband network. Broadband networks can do so much more for public safety because they permit us to add applications over and above LMR. All the ones mentioned above are good examples. Pennsylvania is moving in this direction now. We have an 800 MHz network with a VHF overlay. We are building a UHF overlay and have submitted a grant to run both commercial and public safety broadband – all on the same network. We run automatic vehicle location services and provide data services to the state police. This is the future of public safety LMR systems. It's not just voice anymore.

What is the current thinking on solutions to the geo-location problem in NG 911?

By the word 'problem' I assume you mean the issue of caller location and routing to the correct PSAP VOIP calls. It has been several years since I was in charge of a 911 center (Philadelphia) and the scope of the VOIP issue was just being understood so I will defer an answer to this question as I have been away from this subject for awhile.

Sincerely,

Charles J. Brennan
Deputy Secretary of Administration
Office of Public Safety Radio Services
Commonwealth of Pennsylvania

717-772-8006

chabrennan@state.pa.us